NOTICE

U.S. Department of Transportation
Federal Aviation Administration

N 8110.92

01/16/01

Cancellation Date: 01/16/02

SUBJ: GUIDELINES FOR APPLYING THE RTCA/DO-178B LEVEL D CRITERIA TO PREVIOUSLY DEVELOPED SOFTWARE (PDS)

1. PURPOSE. This notice provides guidelines to Aircraft Certification Office (ACO) engineers and Designated Engineering Representatives (DER) regarding the application of RTCA/DO-178B, "Software Considerations in Airborne Systems and Equipment Certification," to previously developed software (PDS) that has been categorized to contribute to at most a minor failure condition on the aircraft. Advisory Circular (AC) 20-115B recognizes DO-178B as an acceptable means of compliance for the evaluation of software in airborne systems and equipment. DO-178B assigns a software level of D to any software that can cause or contribute to no more than a minor aircraft failure condition. However, the application of the objectives associated with Level D software are frequently misinterpreted, especially when applied to software that was not originally approved using DO-178B (i.e., PDS). This notice should be used to apply DO-178B to PDS that is categorized as Level D.

2. DISTRIBUTION. This notice is distributed to the branch level in Washington Headquarters Aircraft Certification Service, section level in all Aircraft Certification Directorates, all National Resource Specialists (NRS), all Aircraft Certification Offices (ACO), all Manufacturing Inspection Offices (MIO), all Manufacturing Inspection District and Satellite Offices (MIDO/MISO), and all Flight Standards District Offices (FSDO). Additional limited distribution should be made to the Air Carrier District Offices, the Aeronautical Quality Assurance Field Offices, and the Federal Aviation Administration (FAA) Academy.

3. RELATED PUBLICATIONS.

a. Advisory Circular 20-115B, "RTCA, Inc. Document RTCA/DO-178B," dated January 11, 1993.

b. RTCA, Incorporated, document RTCA/DO-178B, "Software Considerations in Airborne Systems and Equipment Certification," dated December 1, 1992.

4. BACKGROUND. On January 11, 1993, the FAA issued AC 20-115B which recognizes DO-178B as a means of demonstrating compliance to regulations for the software aspects of aircraft systems. DO-178B provides for five different levels of software based on the software's contribution to potential failure conditions. These software levels represent differing levels of development process rigor based on the severity of the potential failure conditions to which the software can contribute. Level D is assigned to software that can cause or contribute to no more than a minor

aircraft failure condition. DO-178B contains 28 objectives for Level D software that should be satisfied before approval is granted. To be consistent with a minor aircraft failure condition, the intent of Level D software objectives is to provide a thorough investigation of the functional behavior of the software and to provide the necessary configuration control. However, some of the required objectives for Level D have been misinterpreted when considered with the overall objective of establishing correct functional behavior. Due to confusion over Level D objectives, application of DO-178B for these systems has not been consistent over different projects. Many developers may decide to do more than the stated requirements for Level D; however, this notice concentrates on the minimum requirements. Proper application of Level D objectives permits the use of PDS, which is software that was not originally approved using DO-178B (e.g., Commercial-off-the-shelf (COTS) software, software developed using military standards, software developed using DO-178 or DO-178A, software developed using other industry standards). Reference Section 12.1 of DO-178B for additional guidance for using PDS. In particular, Section 12.1.4 should be referenced for additional considerations when upgrading a previous development baseline. While this notice addresses PDS, the guidelines may also be applicable for other software required to meet the DO-178B Level D objectives.

5. DISCUSSION. A consistent interpretation of DO-178B for Level D software is important for the approval of PDS software. Of the 28 objectives found in DO-178B for Level D software, experience has shown that there are five objectives that are frequently misinterpreted. One of the objectives is related to integral processes; the remaining four objectives are related to source code, software architecture, and low-level requirement definitions. The discussion presented in this section is applicable to any DO-178B, Level D, software approval. Section 6 provides specific procedures for the approval of Level D PDS.

a. Objective 1 in DO-178B, Annex A, Table A-1, "Software development and integral processes activities are defined." A number of field-experience comments point to the absence of any requirement to comply with Objective 6 in DO-178B, Annex A, Table A-1 which states "Software Plans comply with this document (i.e., DO-178B)" and have concluded that there should not be a requirement to comply with Objective 1 which states "Software development and integral processes activities are defined." However, Objective 1 ensures that even for Level D software: (1) there are some plans (e.g., Plan for Software Aspects of Certification, Software Development Plan, Software Configuration Management Plan, Software Quality Assurance Plan, Software Verification Plan), even if the plans themselves do not comply with DO-178B, and (2) those plans are followed (see Objective 1 in DO-178B, Annex A, Table A-9). Additionally, the plans should enable compliance to the DO-178B objectives applicable for Level D software.

b. Objective 4 in DO-178B, Annex A, Table A-2, "Low-level requirements are developed." For Level D software, the intent of this objective is to assure that the low-level requirements and architecture (software design) are defined. However, Table A-4 objectives related to the architecture and low-level requirements require no explicit verification of the software architecture and low-level requirements. Therefore, Objective 4 of Table A-2 is satisfied implicitly by satisfying Objectives 1 and 2 in DO-178B, Annex A, Table A-6. The satisfaction of Objectives 1 and 2 demonstrate that the executable code complies with and is robust with high-level requirements. Since there is no

requirement to ensure that the executable code is compatible with the low-level requirements, it is not necessary to ensure that the low-level requirements are traceable to the high-level requirements.

c. Objective 3 in DO-178B, Annex A, Table A-2, "Software architecture is developed." The logic as applied in paragraph 5(b) above may be applied to Objective 3 (i.e., Objective 3 is implicitly satisfied by other objectives and does not need to be explicitly satisfied for Level D PDS, since Table A-4, Objectives 8 through 12, do not require verification of the software architecture).

d. Objective 5 in DO-178B, Annex A, Table A-2, "Derived low-level requirements are defined" The referenced paragraph for Objective 5 (i.e., paragraph 5.2.1b) states that "Derived low-level requirements are provided to the system safety assessment process," rather than just "defined." As with the low-level requirements and software architecture, there is no explicit verification of derived low-level requirements for Level D software. The satisfaction of this objective is implied by satisfying Objective 2 in DO-178B, Annex A, Table A-2, "Derived high-level requirements are defined" and the associated verification of high-level requirements.

e. Objective 6 in DO-178B Annex A, Table A-2, "Source code is developed." The actual DO-178B referenced text for Objective 6 (i.e., paragraph 5.3.1a) states, "Source code is developed that is traceable, verifiable, consistent, and correctly implements low-level requirements." However, according to Annex A, Table A-5, there are no verification objectives for Level D source code. Therefore, there is no requirement to establish consistency between source code, low-level requirements, and high-level requirements. The consistency requirement is between the executable code and the high-level requirements for Level D. The objective is for the executable code to meet all of the functional verification elements. Furthermore, the existence of object code implies the existence of source code so that Objective 6 of DO-178B, Annex A, Table A-2 is reasonably covered by satisfying other objectives (i.e., Objectives 1 and 2 of Table A-2; Objective 2 of Table A-3; Objectives 1 and 2 of Table A-6; and Objective 3 of Table A-7) for level D software.

6. PROCEDURES. For a project involving approvals of Level D PDS, the cognizant ACO engineer and/or the DER (if authorized) should follow the procedures listed below:

a. Software reviewers should review the software plans to assure that: (1) some plans exist (e.g., Plan for Software Aspects of Certification, Software Development Plan, Software Configuration Management Plan, Software Quality Assurance Plan, Software Verification Plan); (2) those plans are followed (reference DO-178B, Annex A, Table A-9, Objective 1); and (3) the plans enable compliance to DO-178B objectives for Level D software.

b. Software reviewers can ensure that low-level requirements, software architecture, derived low-level requirements, and source code are defined and exist for Level D software; however, software reviewer should not assess the quality or compliance of these artifacts to DO-178B objectives and software life cycle data content requirements. The intent for Level D of these objectives will be satisfied by the objectives for Level D for Tables A-6 and A-7.

c. When evaluating the PDS, the following steps should be followed:

(1) The applicant should verify that a failure condition or malfunction of the Level D software can contribute to no more than a minor failure condition.

(2) The applicant should identify the functions to be used from the PDS.

(3) The applicant should ensure that the PDS can not result in an unacceptable failure condition in the target application.

d. In the case where multiple software levels for a given system and/or component exist, the protection and associated mechanisms between the different software levels should be verified to meet the objectives of the highest level of software associated with the system component. This can occur when there are multiple functions in a component (e.g., maintenance and navigation) or when there are different categorizations of types of failure conditions, such as loss of function versus a corrupted function (e.g., misleading display data). An example of the latter case is a navigation system supported by a PDS operating system. The loss of the navigation function can be shown to produce only a minor aircraft failure condition, whereas misleading navigation is usually considered to be a major aircraft failure condition. If the navigation function is protected (partitioned) from the operating system in such a way that any failure of the operating system can be shown to produce only a loss of function, then the operating system only needs to be evaluated to Level D criteria. However, the applicant needs to verify that indeed the operating system can only contribute to loss of navigation function and not to a misleading navigation failure condition. In this case, part of the development effort would be to demonstrate that the PDS can be shown to meet all the Level D objectives, as outlined above.

e. It is theoretically possible for Level D software to operate in conjunction with software of other levels. In this case a thorough protection/partitioning analysis should be performed in conjunction with the system safety assessment. However, discussion of protection/partitioning is outside the scope of this notice and will not be further discussed.

f. See DO-178B, Section 12.1, for additional guidance on the use of PDS.

7. CONCLUSION. The information and procedures described in this notice constitute a means to consistently interpret the guidelines in DO-178B for approving PDS that has been assessed to have a software level of D. The guidelines may also be applicable to other Level D software. This notice does not replace or supersede AC 20-115B or DO-178B.

James C. Jones
Manager, Aircraft Engineering Division
Aircraft Certification Service